Buffer errors

CWE-118	Incorrect Access of Indexable Resource ('Range Error')
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-123	Write-what-where Condition
CWE-124	Buffer Underwrite ('Buffer Underflow')
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-127	Buffer Under-read
CWE-129	Improper Validation of Array Index
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-131	Incorrect Calculation of Buffer Size
CWE-680	Integer Overflow to Buffer Overflow
CWE-785	Use of Path Manipulation Function without Maximum-sized Buffer
CWE-786	Access of Memory Location Before Start of Buffer
CWE-787	Out-of-bounds Write
CWE-788	Access of Memory Location After End of Buffer
CWE-805	Buffer Access with Incorrect Length Value
CWE-806	Buffer Access Using Size of Source Buffer
CWE-823	Use of Out-of-range Pointer Offset

Numeric errors

CWE-128	Wrap-around Error
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-192	Integer Coercion Error
CWE-194	Unexpected Sign Extension
CWE-195	Signed to Unsigned Conversion Error
CWE-196	Unsigned to Signed Conversion Error
CWE-197	Numeric Truncation Error
CWE-234	Failure to Handle Missing Parameter
CWE-369	Divide By Zero
CWE-456	Missing Initialization of a Variable
CWE-457	Use of Uninitialized Variable
CWE-665	Improper Initialization
CWE-681	Incorrect Conversion between Numeric Types
CWE-824	Access of Uninitialized Pointer

Resource management

CWE-188	Reliance on Data/Memory Layout
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release
CWE-415	Double Free
CWE-416	Use After Free
CWE-463	Deletion of Data Structure Sentinel
CWE-467	Use of sizeof() on a Pointer Type
CWE-468	Incorrect Pointer Scaling
CWE-476	NULL Pointer Dereference
CWE-562	Return of Stack Variable Address
CWE-587	Assignment of a Fixed Address to a Pointer
CWE-588	Attempt to Access Child of a Non-structure Pointer
CWE-590	Free of Memory not on the Heap

CWE-672	Operation on a Resource after Expiration or Release
CWE-690	Unchecked Return Value to NULL Pointer Dereference
CWE-761	Free of Pointer not at Start of Buffer
CWE-762	Mismatched Memory Management Routines
CWE-763	Release of Invalid Pointer or Reference
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-771	Missing Reference to Active Allocated Resource
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-789	Uncontrolled Memory Allocation
CWE-825	Expired Pointer Dereference
CWE-908	Use of Uninitialized Resource
CWE-909	Missing Initialization of Resource
CWE-911	Improper Update of Reference Count

Information leakage

CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-201	Exposure of Sensitive Information Through Sent Data
CWE-202	Exposure of Sensitive Information Through Data Queries
CWE-203	Observable Discrepancy
CWE-205	Observable Behavioral Discrepancy
CWE-206	Observable Internal Behavioral Discrepancy
CWE-212	Improper Removal of Sensitive Information Before Storage or Transfer
CWE-226	Sensitive Information Uncleared in Resource Before Release for Reuse
CWE-244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')
CWE-524	Use of Cache Containing Sensitive Information

Injection

INJ-1	Untrusted Data Accessed as Machine Language Instructions
INJ-2	Untrusted Data Accessed as Heap Metadata
INJ-3	Untrusted Data Accessed as Trusted Data

Privileges, permissions, and access control

PPAC-1	Missing authorization in privileged resource access; Related to CWEs 284, 285, 288, 668, 669, 862, and 863
PPAC-2	Reliance on OS and software for authentication; Related to CWEs 284, 287, and 288
PPAC-3	Security exceptions are not logged to a privileged location; Related to CWE 284

Hardware/system-on-chip implementation errors

CWE-208	Observable Timing Discrepancy
CWE-385	Covert Timing Channel
CWE-920	Improper Restriction of Power Consumption
CWE-1037	Processor Optimization Removal or Modification of Security-critical Code
CWE-1050	Excessive Platform Resource Consumption within a Loop
CWE-1189	Improper Isolation of Shared Resources on System-on-Chip (SoC)
CWE-1193	Power-On of Untrusted Execution Core Before Enabling Fabric Access Control
CWE-1209	Failure to Disable Reserved Bits
CWE-1220	Insufficient Granularity of Access Control
CWE-1221	Incorrect Register Defaults or Module Parameters
CWE-1222	Insufficient Granularity of Address Regions Protected by Register Locks
CWE-1223	Race Condition for Write-Once Attributes
CWE-1224	Improper Restriction of Write-Once Bit Fields
CWE-1231	Improper Implementation of Lock Protection Registers
CWE-1232	Improper Lock Behavior After Power State Transition
CWE-1233	Improper Hardware Lock Protection for Security Sensitive Controls
CWE-1234	Hardware Internal or Debug Modes Allow Override of Locks

CWE-1239	Improper Zeroization of Hardware Register
CWE-1240	Use of a Risky Cryptographic Primitive
CWE-1241	Use of Predictable Algorithm in Random Number Generator
CWE-1242	Inclusion of Undocumented Features or Chicken Bits
CWE-1243	Exposure of Security-Sensitive Fuse Values During Debug
CWE-1245	Improper Finite State Machines (FSMs) in Hardware Logic
CWE-1246	Improper Write Handling in Limited-write Non-Volatile Memories
CWE-1251	Mirrored Regions with Different Values
CWE-1252	CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations
CWE-1253	Incorrect Selection of Fuse Values
CWE-1254	Incorrect Comparison Logic Granularity
CWE-1256	Hardware Features Enable Physical Attacks from Software
CWE-1257	Improper Access Control Applied to Mirrored or Aliased Memory Regions
CWE-1259	Improper Protection of Security Identifiers
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1261	Improper Handling of Single Event Upsets
CWE-1262	Register Interface Allows Software Access to Sensitive Data or Security Settings
CWE-1264	Hardware Logic with Insecure De-Synchronization between Control and Data Channels
CWE-1268	Agents Included in Control Policy are not Contained in Less-Privileged Policy
CWE-1270	Generation of Incorrect Security Identifiers
CWE-1271	Missing Known Value on Reset for Registers Holding Security Settings
CWE-1272	Debug/Power State Transitions Leak Information
CWE-1273	Device Unlock Credential Sharing
CWE-1274	Insufficient Protections on the Volatile Memory Containing Boot Code
CWE-1276	Hardware Block Incorrectly Connected to Larger System
CWE-1277	Firmware Not Updateable
CWE-1279	Cryptographic Primitives used without Successful Self-Test
CWE-1280	Access Control Check Implemented After Asset is Accessed
CWE-1281	Sequence of Processor Instructions Leads to Unexpected Behavior (Halt and Catch Fire)
CWE-1282	Assumed-Immutable Data Stored in Writable Memory
CWE-1283	Mutable Attestation or Measurement Reporting Data

[1] CWE definitions from the MITRE Common Weakness Enumeration (CWE) version 4.1

[2] INJ- and PPAC- descriptions created for the SSITH program as concrete examples of weaknesses in the category